UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

***IN RE* ADVOCATE AURORA HEALTH PIXEL LITIGATION**

SHYANNE JOHN, Plaintiffs, v. ADVOCATE AURORA HEALTH, INC., Defendant.	Case No. 22-CV-1253-JPS
RICHARD WEBSTER, Plaintiffs, v. ADVOCATE AURORA HEALTH, INC., Defendant.	Case No. 22-CV-1278-JPS
DEANNA DANGER, Plaintiffs, v. ADVOCATE AURORA HEALTH, INC., Defendant.	Case No. 22-CV-1305-JPS

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Shyanne John, Richard Webster, Deanna Danger, James Gabriel, Katrina Jones, Derrick Harris, Amber Smith, and Bonnie Laporte (collectively, "Plaintiffs"), on behalf of themselves and on behalf of all others similarly situated ("Class Members"), bring this Consolidated Amended Class Complaint against Advocate Aurora Health, Inc. ("Advocate" or "Defendant") and allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this case to address Defendant's transmission and disclosure of Plaintiffs' and Class Members' confidential personally identifiable information ("PII") and protected health information ("PHI") (collectively referred to as "Private Information" or "PII and PHI") to Meta Platforms, Inc. d/b/a Meta ("Facebook") and/or Google LLC d/b/a Google ("Google") via a tracking pixel ("Tracking Pixel" or "Pixel") installed on Defendant's website, LiveWell App, and MyChart Portal (collectively referred to as "Website").

2. Plaintiffs' and Class Members' Private Information unlawfully intercepted and transmitted by Defendant includes the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about provider; types of appointments or procedures; communications between patients and others through MyChart, which may have included first and last names and medical record numbers; insurance information; and, if a patient had a proxy MyChart account, the first name and the first name of the proxy.

3. According to its report submitted to the United States Department of Health and Human Services, Defendant admits that the Private Information of at least 3,000,000 individuals

was improperly and unlawfully disclosed to Facebook and Google without those individuals' knowledge or consent.[1]

4. Defendant is a non-profit healthcare system located in Illinois and Wisconsin. It has 26 hospitals, 500 sites of care, and 75,000 employees.[2] Defendant is one of the largest healthcare providers in the United States.

5. In order to provide medical treatment and care, Defendant collects and stores patients' Private Information and medical records. In doing so, Defendant has statutory, regulatory, contractual, fiduciary, and common law duties to safeguard that Private Information from disclosure and ensure that it remains private and confidential. Defendant is duty bound to maintain the confidentiality of patient medical records and information and is further required to do so by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and by Wisconsin and Illinois statutes.[3]

6. Plaintiffs and Class Members are individuals who are seeking or have sought medical services and/or treatment from Defendant. Defendant advertises its online services on its Website, including the LiveWell App and MyChart Portal, to assist patients with their medical care. Based on Defendant's encouragement that patients use its online services, Plaintiffs used Defendant's Website to search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from their healthcare providers, receive lab results, review medical records, and exchange insurance information.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Nov. 14, 2022).
[2] https://www.aurorahealthcare.org/about-aurora/ (last visited: January 12, 2023).
[3] The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996), ("HIPAA"), and regulations of the United States Department of Health and Services ("HHS") promulgated thereunder, are designed to protect the confidentiality and guard against the unauthorized disclosure of medical records, patient health care information, and other individually identifiable healthcare information.

7. Defendant's Privacy Policies ("Privacy Policies") unequivocally state that Defendant will not share Plaintiffs' and Class Members' Private Information for marketing purposes unless patients provide written permission.[4]

8. As explained below, however, Defendant did disclose Plaintiffs' and Class Members' Private Information via the Tracking Pixel to third parties, such as Facebook and Google. Defendant's disclosure of Plaintiffs' and Class Members' Private Information constitutes a gross violation of common law and statutory data privacy laws.

9. Defendant did not acknowledge the Tracking Pixel and its widespread and blatant disclosures of Plaintiffs' and Class Members' Private Information until on or around October 22, 2022.

10. On or around October 22, 2022, Defendant posted a Statement (hereinafter referred to as the "Notice of Data Security Incident") on its website, which states the following:

> Advocate Aurora Health is writing to provide transparency in its previous use of the Internet tracking technologies, such as Google and Meta (Facebook), that we and many others in our industry had implemented to understand how patients and others interact with our websites. These technologies disclose certain details about interactions with our websites, particularly for users that are concurrently logged into their Google or Facebook accounts and have shared their identity and other surfing habits with these companies. When using some Advocate Aurora Health sites, certain protected health information ("PHI") would be disclosed in particular circumstances to specific vendors because of pixels on our websites or applications.
>
> **What happened?**
> In an effort to deliver high quality services to its community, Advocate Aurora Health uses the services of several third-party vendors to measure and evaluate information concerning the trends and preferences of its patients as they use our websites. To do so, pieces of code known as "pixels" were included on certain of our websites or applications. These pixels or similar technologies were designed to gather information that we review in aggregate so that we can better understand patient needs and preferences to provide needed care to our patient population. We learned that pixels or similar technologies installed on our patient portals available through MyChart and LiveWell websites and applications, as well as on some of

[4] *See* https://www.advocatehealth.com/privacy-policy/?_ga=2.190713003.182618276.1583955525-240549872.1583955525 (last visited: January 23, 2023).

our scheduling widgets, transmitted certain patient information to the third-party vendors that provided us with the pixel technology. We have disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors.

How do I know If I was affected?
Out of an abundance of caution, Advocate Aurora Health has decided to assume that all patients with an Advocate Aurora Health MyChart account (including users of the LiveWell application), as well as any patients who used scheduling widgets on Advocate Aurora Health's platforms, may have been affected. Users may have been impacted differently based on their choice of browser; the configuration of their browsers; their blocking, clearing or use of cookies; whether they have Facebook or Google accounts; whether they were logged into Facebook or Google; and the specific actions taken on the platform by the user.

What information was involved?
The following information may have been involved: your IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; type of appointment or procedure; communications between you and others through MyChart, which may have included your first and last name and your medical record number; information about whether you had insurance; and, if you had a proxy MyChart account, your first name and the first name of your proxy. Based on our investigation, no social security number, financial account, credit card, or debit card information was involved in this incident.

11. Parsing out Defendant's Notice of Data Security Incident, Defendant has admitted that its Website, including its LiveWell App and MyChart Portal, contain a Tracking Pixel that secretly enabled the unauthorized transmission and disclosure of Plaintiffs' and Class Members' Private Information to third parties such as Facebook or Google.

12. Defendant also acknowledged the Notice of Security Incident pertains to "all patients with an Advocate Aurora Health MyChart account (including users of the LiveWell application), as well as any patients who used scheduling widgets on Advocate Aurora Health's platforms, may have been affected."

13. Third parties, like Facebook or Google, in turn, use Plaintiffs' and Class Members' Private Information to target advertisements to Plaintiffs and Class Members based on the Private Information disclosed by Plaintiffs and Class Members to Defendant.

14. Accordingly, the purpose of this lawsuit is to protect Plaintiffs' and Class Members' right to protect their Private Information and seek remedies for the harm caused by Defendant's intentional, reckless, or negligent disclosure to third parties, such as Facebook or Google.

BACKGROUND

15. When an individual visits Defendant's Website and submits Private Information to Defendant, its Tracking Pixel transmits that Private Information to third parties, such as Facebook and Google. A pixel is a piece of code that "tracks the people and [the] type of actions they take."[5] Pixels are routinely used to target specific customers by utilizing the data gathered through Defendant's pixel to build profiles for the purposes of retargeting[6] and future marketing.

16. For instance, with respect to Facebook, the persistent Facebook Pixel on Defendant's Website causes that individual's unique and persistent Facebook ID ("FID") to be transmitted alongside other Private Information that is sent to Facebook.

17. Upon information and belief, Defendant utilized the Pixel data to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients. In other words, Defendant implemented the Tracking Pixel to bolster its profits.

[5] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting (last visited Nov. 14, 2022).
[6] "Retargeting" or "remarketing" is a form of advertising that displays ads or sends emails to previous visitors of a particular website who did not "covert" the visit into a sale or otherwise meet a marketing goal of the website owner.

18. Pixels are routinely used to target advertising to specific customers by utilizing the data gathered through the pixel to build profiles for the purposes of retargeting and future marketing.

19. In this context, the Tracking Pixel is designed to report to third parties data gathered about the web page currently visited and any information to/from the User to the web page. In other words, a pixel creates a link – hidden from the website's user – that transfers information sent to/from the web page to the third party.

20. Operating as designed, Defendant's Tracking Pixel allowed the Private Information that Plaintiffs and Class Members submitted to Defendant to be unlawfully disclosed to third parties.

21. For example, when Plaintiffs or a Class Member accessed Defendant's Website hosting the Pixel, the Pixel software directed Plaintiffs' or Class Members' browser to send a message to the third party's servers. The information sent to third parties by Defendant included the Private Information that Plaintiffs and Class Members submitted to Defendant's Website, including, for example, the type and date of a medical appointment and physician. Such Private Information would allow the third party (e.g., Facebook or Google) to know that a specific patient was seeking confidential medical care and the type of medical care being sought. This disclosure would also allow a third party to reasonably infer that a specific patient was being treated for a specific type of medical condition such as cancer, pregnancy, or HIV.

22. The third party, in turn, sells Plaintiffs' and Class Members' Private Information to third-party marketers who online target[7] Plaintiffs and Class Members based on communications obtained via the Tracking Pixel.

23. Plaintiffs submitted medical information to Defendant's Website, including the LiveWell App and MyChart Portal, and used the Website to search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from their healthcare providers, receive lab results, review medical records, and exchange insurance information.

24. Via the Tracking Pixel, Defendant transmitted this Private Information to third parties, such as Facebook and Google.

25. Defendant regularly encouraged Plaintiffs and Class Members to use its digital tools, including its Website, LiveWell App, and MyChart Portal, to receive healthcare services. In doing so, Defendant also directed Plaintiffs and Class Members to its Privacy Policies, which preclude the transmission or disclosure of Private Information to unauthorized third parties, such as Facebook or Google.

26. Plaintiffs and Class Members provided Private Information to Defendant in order to receive medical services and with the reasonable expectation that Defendant would protect their Private Information.

27. At all times that Plaintiffs and Class Members visited and utilized Defendant's Website, they had a reasonable expectation of privacy in the Private Information collected through Defendant's Website, including that it would remain secure and protected and only utilized for

[7] "Online Targeting" is "a process that refers to creating advertisement elements that specifically reach out to prospects and customers interested in offerings. A target audience has certain traits, demographics, and other characteristics, based on products or services the advertiser is promoting." *See* https://digitalmarketinggroup.com/a-guide-to-online-targeting-which-works-for-your-business/ (last visited: January 23, 2023).

medical purposes. Plaintiffs' and Class Members' expectations were entirely reasonable because (1) they are patients; and (2) Defendant is a healthcare provider which is required by common and statutory law to protect its patients' Private Information. Moreover, Plaintiffs and Class Members also relied on Defendant's Privacy Policies, which do not permit the transmission or disclosure of Plaintiffs' and Class Members' Private Information to unauthorized third parties.

28. Defendant further made express and implied promises to protect Plaintiffs' and Class Members' Private Information and maintain the privacy and confidentiality of communications that patients exchange with Defendant.

29. Defendant owed common law, contractual, statutory, and regulatory duties to keep Plaintiffs' and Class Members' Private Information safe, secure, and confidential. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized disclosure.

30. However, as set forth more fully below, Defendant failed in its obligations and promises by utilizing the Tracking Pixel on its Website knowing that such technology would transmit and disclose Plaintiffs' and Class Members' Private Information to unauthorized third parties.

31. The exposed Private Information of Plaintiffs and Class Members can—and likely will—be further disseminated to additional third parties utilizing the data for retargeting or to insurance companies utilizing the information to set insurance rates.

32. While Defendant willfully and intentionally incorporated the Tracking Pixel into its Website, Defendant did not disclose to Plaintiffs or Class Members that it shared their sensitive and confidential communications via the Tracking Pixel to Facebook or Google until on or around

October 22, 2022.[8] As a result, Plaintiffs and Class Members were unaware that their Private Information was being surreptitiously transmitted and/or disclosed to Facebook and Google as they communicated with their healthcare provider via the Website.

33. Defendant breached its obligations in one or more of the following ways: (i) failing to adequately review its marketing programs and web based technology to ensure Defendant's Website was safe and secure; (ii) failing to remove or disengage technology that was known and designed to share web-users' information; (iii) failing to obtain the consent of Plaintiffs and Class Members to disclose their Private Information to Facebook, Google, or others; (iv) failing to take steps to block the transmission of Plaintiffs' and Class Members' Private Information through Tracking Pixels; (v) failing to warn Plaintiffs and Class Members; and (vi) otherwise failing to design and monitor its Website to maintain the confidentiality and integrity of patient Private Information.

34. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy, (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Tracking Pixel, (iii) loss of benefit of the bargain, (iv) diminution of value of the Private Information, (v) statutory damages, and (vi) the continued and ongoing risk of exposure of their Private Information.

35. Plaintiffs seek to remedy these harms and bring causes of action for (1) invasion of privacy; (2) unjust enrichment; (3) breach of implied contract; (4) breach of confidence; (5) violations of the Electronics Communication Privacy Act ("ECPA") 18 U.S.C. § 2511(1) - unauthorized interception, use, and disclosure; (6) violations of ECPA, 18 U.S.C. § 2511(3)(a) - unauthorized interception, use, and disclosure; (7) violations of Title II of the ECPA, 18 U.S.C.

[8] https://www.wpr.org/data-breach-advocate-aurora-health-system-may-have-exposed-3m-patients-information (Last Visited: January 20, 2023).

§ 2702, *et seq.*, - Stored Communications Act; (8) violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq.*; (9) failure to maintain Confidentiality of Patient Healthcare Records Act under Wisconsin law, Wis. Stat. § 146.81, *et seq.*; (10) violations of the Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§ 100.18, *et seq.*; (11) failure to maintain Confidentiality of Patient Healthcare Records Act under Illinois law, § 410 ILCS 50, *et seq.*; and (12) violations of the Illinois Consumer Fraud and Deceptive Business Practices Act.

PARTIES

Plaintiff Shyanne John

36. Plaintiff Shyanne John is a citizen and resident of Wisconsin.

37. Plaintiff John has received healthcare services since 1999 at one of the hospitals in Defendant's network and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

38. Plaintiff John has been using Defendant's Website, including the LiveWell App and MyChart Portal, since 2018.

39. Plaintiff John used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

40. Plaintiff John has been a Facebook user since 2013.

41. Plaintiff John accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

42. As Defendant's patient, Plaintiff John reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff John also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff John would not have disclosed her Private Information to Defendant.

43. During her time as a patient, Plaintiff John never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

44. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff John's Private Information to third parties, such as Facebook and Google.

Plaintiff Richard Webster

45. Plaintiff Richard Webster is a citizen and resident of Wisconsin.

46. Plaintiff Webster received healthcare services commencing in 2008 from one of the hospitals in Defendant's network and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

47. Plaintiff Webster has been using Defendant's Website, including the LiveWell App and MyChart Portal, since at least 2014.

48. Plaintiff Webster used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

49. Plaintiff Webster has been a Facebook user since 2012.

50. Plaintiff Webster accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

51. As a patient in Defendant's healthcare network, Plaintiff Webster reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Webster also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Webster would not have disclosed his Private Information to Defendant.

52. During his time as a patient, Plaintiff Webster never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

53. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Webster's Private Information to third parties, such as Facebook and Google.

Plaintiff Deanna Danger

54. Plaintiff Deanna Danger is a citizen and resident of Wisconsin.

55. Plaintiff Danger has received healthcare services since 2006 from one of the hospitals in Defendant's network and has used Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

56. Plaintiff Danger has been using Defendant's Website, including the LiveWell App and MyChart Portal, since 2013.

57. Plaintiff Danger used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and

procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

58. Plaintiff Danger has been a Facebook user since 2011.

59. Plaintiff Danger accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

60. As a patient in Defendant's healthcare network, Plaintiff Danger reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Danger also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Danger would not have disclosed her Private Information to Defendant.

61. During her time as a patient, Plaintiff Danger never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

62. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Danger's Private Information to third parties, such as Facebook and Google.

Plaintiff James Gabriel

63. Plaintiff James Gabriel is a citizen and resident of Wisconsin.

64. Plaintiff Gabriel has received healthcare services from Defendant since the 1970's and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

65. Plaintiff Gabriel has been using Defendant's LiveWell App and MyChart Portal since 2018.

66. Plaintiff Gabriel used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

67. Plaintiff Gabriel has had a Facebook account for the past ten years.

68. Plaintiff Gabriel accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

69. As a patient in Defendant's healthcare network, Plaintiff reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Gabriel also relied on Defendant's Privacy Policies in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Gabriel would not have disclosed his Private Information to Defendant.

70. During his time as a patient, Plaintiff Gabriel never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

71. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Gabriel's Private Information to third parties, such as Facebook and Google.

Plaintiff Katrina Jones

72. Plaintiff Katrina Jones is a citizen and resident of Illinois.

73. Plaintiff Jones has received healthcare services from Defendant since the early 2000s and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

74. Plaintiff Jones has been using Defendant's LiveWell App and MyChart Portal since 2017.

75. Plaintiff Jones used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

76. Plaintiff Jones has been a Facebook user since 2009.

77. Plaintiff Jones accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant or Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

78. As a patient in Defendant's healthcare network, Plaintiff Jones reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Jones also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Jones would not have disclosed her Private Information to Defendant.

79. During her time as a patient, Plaintiff Jones never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

80. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Jones' Private Information to third parties, such as Facebook and Google.

Plaintiff Derrick Harris

81. Plaintiff Derrick Harris is a citizen and resident of Illinois.

82. Plaintiff Harris has received healthcare services from Defendant since 2019 from one of the hospitals in Defendant's network and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

83. Plaintiff Harris has been using Defendant's LiveWell App and MyChart Portal since 2019.

84. Plaintiff Harris used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from his healthcare providers, receive lab results, and review medical records.

85. Plaintiff Harris has been a Facebook user since 2010.

86. Plaintiff Harris accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

87. As a patient in Defendant's healthcare network, Plaintiff Harris reasonably expected that his online communications with Defendant were solely between himself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Harris also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard his Private Information. But for his status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Harris would not have disclosed his Private Information to Defendant.

88. During his time as a patient, Plaintiff Harris never consented to the use of his Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

89. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Jones' Private Information to third parties, such as Facebook and Google.

Plaintiff Amber Smith

90. Plaintiff Amber Smith is a citizen and resident of Illinois.

91. Plaintiff Smith has received healthcare services since 2019 from one of the hospitals in Defendant's network and has relied on Defendant's digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

92. Plaintiff Smith has been using Defendant's LiveWell App since 2019.

93. Plaintiff Smith used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

94. Plaintiff Smith has had a Facebook account since at least 2008.

95. As a patient in Defendant's healthcare network, Plaintiff reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party. Plaintiff Jones also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Smith would not have disclosed her Private Information to Defendant.

96. During her time as a patient, Plaintiff Smith never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

97. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Jones' Private Information to third parties, such as Facebook and Google

Plaintiff Bonnie Laporte

98. Plaintiff Bonnie Laporte is a citizen and resident of Illinois.

99. Plaintiff Laporte has received healthcare services from Defendant since 2014 from one of the hospitals in Defendant's network and has relied on Defendant's Website and digital healthcare platforms to communicate Private Information to Defendant on numerous occasions.

100. Plaintiff Laporte has been using Defendant's LiveWell App and MyChart Portal since 2014.

101. Plaintiff Laporte used Defendant's Website, including the LiveWell App and MyChart, to conduct the following activities: search for physicians, schedule appointments and procedures, receive and discuss medical diagnoses and treatment from her healthcare providers, receive lab results, and review medical records.

102. Plaintiff Laporte has been a Facebook user since 2009.

103. Plaintiff Laporte accessed Defendant's Website, including the LiveWell App and MyChart Portal, to receive healthcare services from Defendant's affiliates at Defendant's direction and with Defendant's encouragement.

104. As a patient in Defendant's healthcare network, Plaintiff Laporte reasonably expected that her online communications with Defendant were solely between herself and Defendant, and that such communications would not be transmitted or intercepted by a third party.

Plaintiff Laporte also relied on Defendant's Privacy Policy in reasonably expecting Defendant would safeguard her Private Information. But for her status as Defendant's patient and Defendant's Privacy Policies, Plaintiff Laporte would not have disclosed her Private Information to Defendant.

105. During her time as a patient, Plaintiff Laporte never consented to the use of her Private Information by third parties or to Defendant enabling third parties, including Facebook or Google, to access or interpret such information.

106. Notwithstanding, through the Tracking Pixel, Defendant transmitted Plaintiff Laporte's Private Information to third parties, such as Facebook and Google.

Defendant Advocate Aurora Health, Inc.

107. Defendant Advocate Aurora Health is a not-for-profit health corporation incorporated in Delaware with its principal place of business at 750 W. Virginia St., P.O. Box 341880, Milwaukee, Wisconsin 53204 and with headquarters in Milwaukee, Wisconsin and Downers Grove, Illinois.

108. Advocate Children's Hospital, Aurora Health Care, Advocate Cancer Institute, Advocate Heart Institute, Advocate Brain and Spine Institute and Orthopedic Center, and other facilities identified herein that were frequented by Plaintiffs, among various others, are all part of the Advocate Health system of health providers. Advocate encourages patients to utilize its Advocate LiveWell patient portal to communicate with their healthcare providers.

JURISDICTION

109. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

110. This Court has federal question jurisdiction under 29 U.S.C. § 1331 because this Complaint alleges violations of the ECPA (28 U.S.C. § 2511, *et seq.*, and 28 U.S.C. § 2702) and the CFAA (18 U.S.C. § 1030, *et seq*).

111. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the many of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

112. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

COMMON FACTUAL ALLEGATIONS

Defendant Improperly Disclosed Plaintiffs' and Class Members' Private Information via the Tracking Pixel.

113. Defendant utilizes its Website to connect Plaintiffs and Class Members to Defendant's digital healthcare platform with the goal of increasing profitability.

114. To accomplish this, Defendant utilized the Tracking Pixel to advertise its services to Plaintiffs and Class Members. The Pixel is a piece of code that Defendant commonly used to secretly track patients by recording their activity and experiences on Defendant's Website and electronic platforms.

115. While seeking and using Defendant's services as a medical provider, and utilizing the Website, Plaintiffs' and Class Members' Private Information was intercepted in real time and then disseminated to Facebook, Google, and potentially to other third parties, via the Pixel that Defendant secretly installed on its Website.

116. Plaintiffs and Class Members did not intend or have any reason to suspect the Private Information would be shared with Facebook, Google, or other third parties, or that Defendant was tracking their every communication and disclosing the same to third parties when

they entered highly sensitive information on Defendant's Website, the LiveWell App, and MyChart portal.

117. Defendant did not disclose to or warn Plaintiffs or Class Members that Defendant used Plaintiffs' and Class Members' confidential electronic medical communications and Private Information for marketing purposes.

118. Defendant tracked Plaintiffs and Class Members' Private Information via the Tracking Pixel.

119. Plaintiffs and Class Members never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information.

120. Upon information and belief, Defendant intercepted and disclosed the following private information to third parties:

a. Plaintiffs' and Class Members' status as medical patients;

b. Plaintiffs' and Class Members' communications with Defendant through its Website;

c. Plaintiffs' and Class Members' medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatments;

121. Defendant deprived Plaintiffs and Class Members of their privacy rights when it: (1) implemented technology (i.e., the Tracking Pixel) that surreptitiously tracked, recorded, and disclosed Plaintiffs' and other online patients' confidential communications and Private Information; (2) disclosed patients' protected information to Facebook, Google, and/or other unauthorized third-parties; and (3) undertook this pattern of conduct without notifying Plaintiffs or Class Members and without obtaining their express written consent.

Defendant's Pixel, Source Code, and Interception of HTTP Requests

122. Web browsers are software applications that allow consumers to navigate the web and view and exchange electronic information and communications over the internet. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (e.g., Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

123. Every website is hosted by a computer "server" that holds the website's contents and through which the entity in charge of the website exchanges communications with Internet users' client devices via their web browsers.

124. Web communications consist of HTTP Requests and HTTP Responses, and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

- **HTTP Request**: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies.
- **Cookies**: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data when visiting one website to an entirely different website.
- **HTTP Response**: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may

consist of a web page, another kind of file, text information, or error codes, among other data.

125. A patient's HTTP Request essentially asks Defendant's Website to retrieve certain information (such as a physician's "Book an Appointment" page), and the HTTP Response renders or loads the requested information in the form of "Markup" (the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Webpage(s)).

126. Every webpage is comprised of Markup and "Source Code." Source Code is a set of instructions invisible to the website's visitor that commands the visitor's browser to take certain actions when the webpage first loads or when a specified event triggers the code.

127. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Pixel is source code that does just that. The Pixel acts much like a traditional wiretap. When patients visit Defendant's website via an HTTP Request to Aurora's server, Defendant's server sends an HTTP Response including the Markup that displays the Webpage visible to the user and Source Code including Defendant's Pixel. Thus, Defendant is in essence handing patients a tapped phone, and once the Webpage is loaded into the patient's browser, the software-based wiretap is quietly waiting for private communications on the Webpage to trigger the tap, which intercepts those communications intended only for Defendant and transmits those communications to third-parties, including Facebook and Google.

128. Third-parties, like Facebook or Google, place third-party cookies in the web browsers of users logged into their services. These cookies uniquely identify the user and are sent with each intercepted communication to ensure the third-party can uniquely identify the patient associated with the Private Information intercepted.

129. With substantial work and technical know-how, internet users can sometimes circumvent this browser-based wiretap technology. This is why third-parties bent on gathering Private Information, like Facebook, implement workarounds that cannot be evaded by savvy users. Facebook's workaround, for example, is called Conversions API. Conversions API is an effective workaround because it does not intercept data communicated from the user's browser. Instead, Conversions API "is designed to create a direct connection between [Web hosts'] marketing data and [Facebook]." Thus, the communications between patients and Defendant, which are necessary to use Defendant's Website, are actually received by Defendant and stored on its server before Conversions API collects and sends the Private Information contained in those communications directly from Defendant to Facebook. Client devices do not have access to host servers and thus cannot prevent (or even detect) this transmission.

130. While there is no way to confirm with certainty that a Web host like Defendant has implemented workarounds like Conversions API without access to the host server, companies like Facebook instruct Defendant to "[u]se the Conversions API in addition to the [] Pixel, and share the same events using both tools," because such a "redundant event setup" allows Defendant "to share website events [with Facebook] that the pixel may lose."[9] Thus, it is reasonable to infer that Facebook's customers who implement the Facebook Pixel in accordance with Facebook's documentation will also implement the Conversions API workaround.

131. The third parties to whom a website transmits data through pixels and associated workarounds do not provide any substantive content relating to the user's communications. Instead, these third parties are typically procured to track user data and communications for marketing purposes of the website owner.

[9] *See* https://www.facebook.com/business/help/308855623839366?id=818859032317965 (last visited Jan. 23, 2023).

132. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its source code to commandeer the user's computing device, causing the device to contemporaneously and invisibly re-direct the users' communications to third parties.

133. In this case, Defendant employed just such a device to intercept, duplicate, and re-direct Plaintiffs' and Class Members' Private Information to third parties like Facebook and Google.

For Example, through Investigation, Plaintiffs uncovered the Facebook Tracking Pixel and Determined that it Regularly Communicated with Facebook during Times that Plaintiffs Communicated Private Information on Defendant's Website.

134. Defendant secretly deployed Facebook's version of a Tracking Pixel, identified as 5725819999876598, on its Website in violation of Defendant's common law, contractual, statutory, and regulatory duties and obligations.

135. The Facebook Pixel, a marketing product, is a "piece of code" that allowed Defendant to "understand the effectiveness of [their] advertising and the actions [patients] take on [their] site."[10] It also allowed Defendant to optimize the delivery of ads, measure cross-device conversions, create custom advertising groups or "audiences," learn about the use of its Website, and decrease advertising and marketing costs.[11]

136. Most importantly, it allowed Facebook to secretly intercept patients' communications on Defendant's Website and patient portal.

Facebook's Platform and its Business Tools

137. Facebook operates the world's largest social media company.

[10] https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022)
[11] *Id.*

138. In 2021, Facebook generated $117 billion in revenue.[12] Roughly 97% of that came from selling advertising space.[13]

139. As a core part of its business, Facebook maintains profiles on users that include the user's real names, locations, email addresses, friends, likes, and communications that Facebook associates with personal identifiers, including IP addresses.

140. Facebook also tracks non-Facebook users through its widespread internet marketing products and source code.

141. Facebook then sells advertising space by highlighting its ability to target users.[14] Facebook can target users so effectively because it surveils user activity both on and off its site.[15] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[16] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[17]

142. Indeed, Facebook utilizes the precise type of information disclosed by Defendant to identify, target, and market products and services to individuals.

143. Advertisers can also build "Custom Audiences."[18] Custom Audiences enable advertisers to reach "people who have already shown interest in [their] business, whether they're

---

[12] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx (last visited Nov. 14, 2022)
[13] *Id.*
[14] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706 (last visited Nov. 14, 2022).
[15] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited Nov. 14, 2022).
[16] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).
[17] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences (last visited Nov. 14, 2022).
[18] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494 (last visited Nov. 14, 2022).

loyal customers or people who have used [their] app or visited [their] website."[19] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[20] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools," including the Facebook Pixel.[21]

144. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[22] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept, collect, view, and use user activity on those platforms.

145. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[23] Facebook's Business Tools

---

[19] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting (last visited Nov. 14, 2022).
[20] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Nov. 14, 2022).
[21] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience https://www.facebook.com/business/help/1474662202748341?id=2469097953376494 (last visited Nov. 14, 2022).
[22] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087 (last visited Nov. 14, 2022).
[23] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/ (last visited Nov.

can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[24] Advertisers can even create their own tracking parameters by building a "custom event." [25]

146. One such Business Tool is the Facebook Pixel. Facebook offers this piece of code to advertisers, like Defendant, to integrate into their websites. As the name implies, the Facebook Pixel "tracks the people and type of actions they take."[26] When a user accesses a website hosting the Facebook Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers at certain times during interaction with the webpage. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Facebook code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and read Defendant's Websites—Defendant's own code, and Facebook's embedded code.

147. Accordingly, during the same transmissions, the Website routinely provides Facebook with its patients' Facebook IDs, IP addresses, and/or device IDs and the other information they input into Defendant's Website, including not only their medical searches and treatment requests but also their home address, zip code, or phone number. This is precisely the type of identifying information that HIPAA requires healthcare providers to de-anonymize to protect the privacy of patients.[27] Plaintiffs' and Class Members identities can be easily determined

---

14, 2022).

[24] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142. (Last visited Nov. 14, 2022)

[25] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/. (Last visited Nov. 14, 2022)

[26] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

[27] https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (Last visited Nov. 14, 2022)

based on the Facebook ID, IP address and/or reverse lookup from the collection of other identifying information that was improperly disclosed.

148. After intercepting and collecting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences. If the Website visitor is also a Facebook user, Facebook will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile, i.e., their real-world identity.

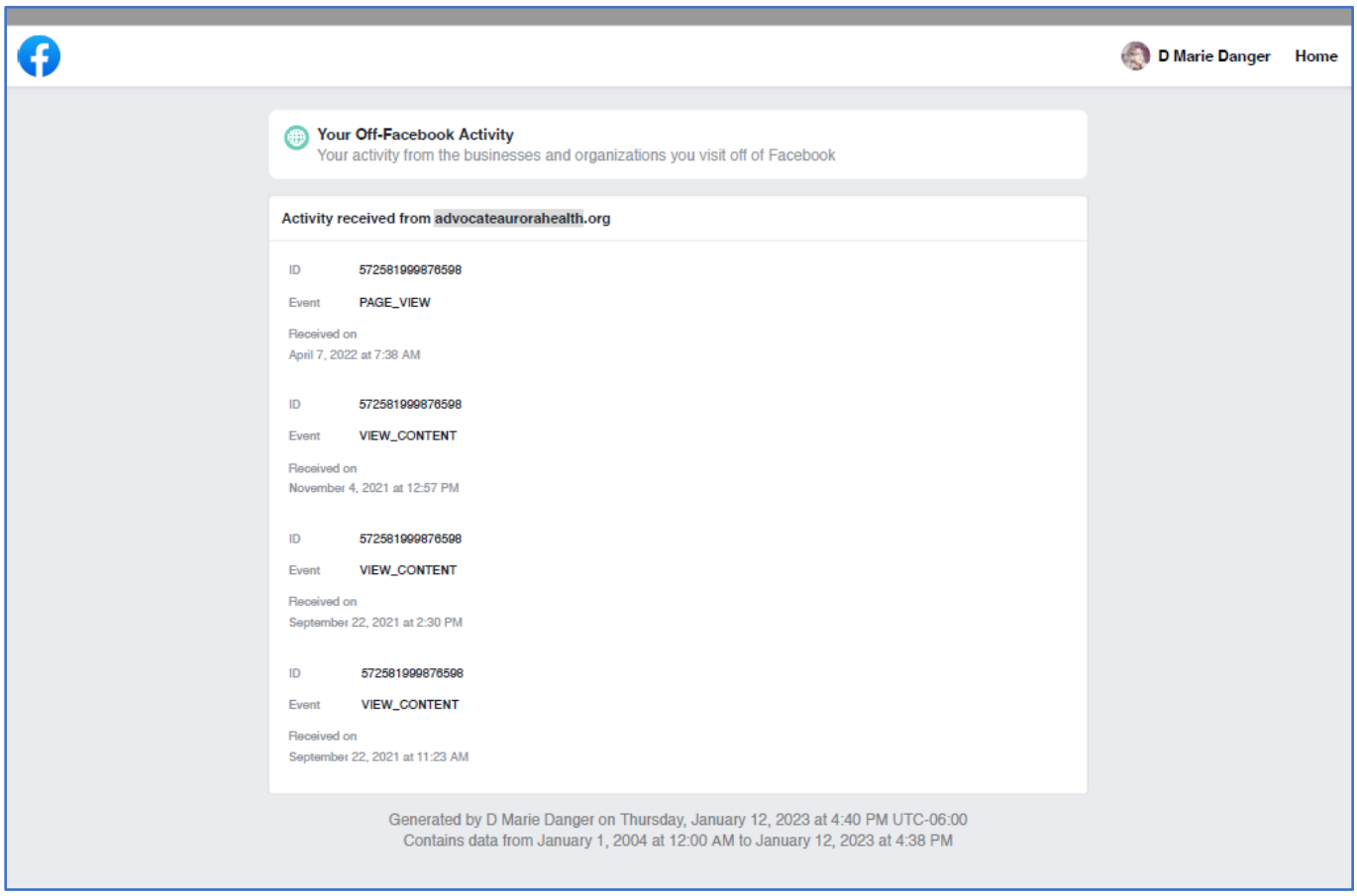
149. A user's FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user's Facebook Profile ID uniquely identifies an individual's Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the user's corresponding Facebook profile.

Plaintiffs Have Specific Evidence of Defendant's Tracking Pixel Communicating with Facebook on dates they submitted Private Information.

150. For example, in this case, Plaintiff Danger's Facebook offsite activity download ("Off-Facebook activity Download")[28] shows the dates and times that Defendant's Tracking Pixel communicated with Plaintiff's Facebook on different pages within Defendant's Website:

[28] The "Off-Facebook activity is a summary of activity that business and organizations share with [Facebook] about [individuals'] interactions, such as visiting [businesses' and organization's] apps or websites." *See* https://www.facebook.com/help/2207256696182627 (Last Visited: January 20, 2023).

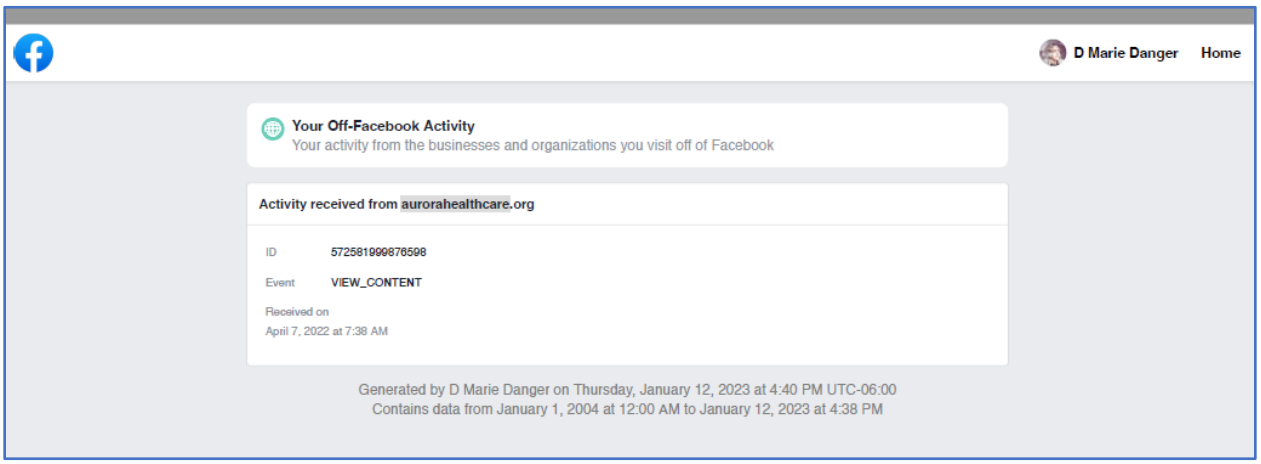
Pixel from www.advocateaurorahealth.org



151. As shown above, Plaintiff Danger's Off-Facebook Download activity shows Defendant's Pixel ID Number 5725819999876598 was contained in Defendant's webpage (www.advocateaurorahealth.org) and communicated with Plaintiff Danger's Facebook on the following dates and times:

- September 22, 2021 at 11:23 am
- September 22, 2021 at 2:30 pm
- November 4, 2021 at 12:57 pm; and
- April 7, 2022 at 7:38 am

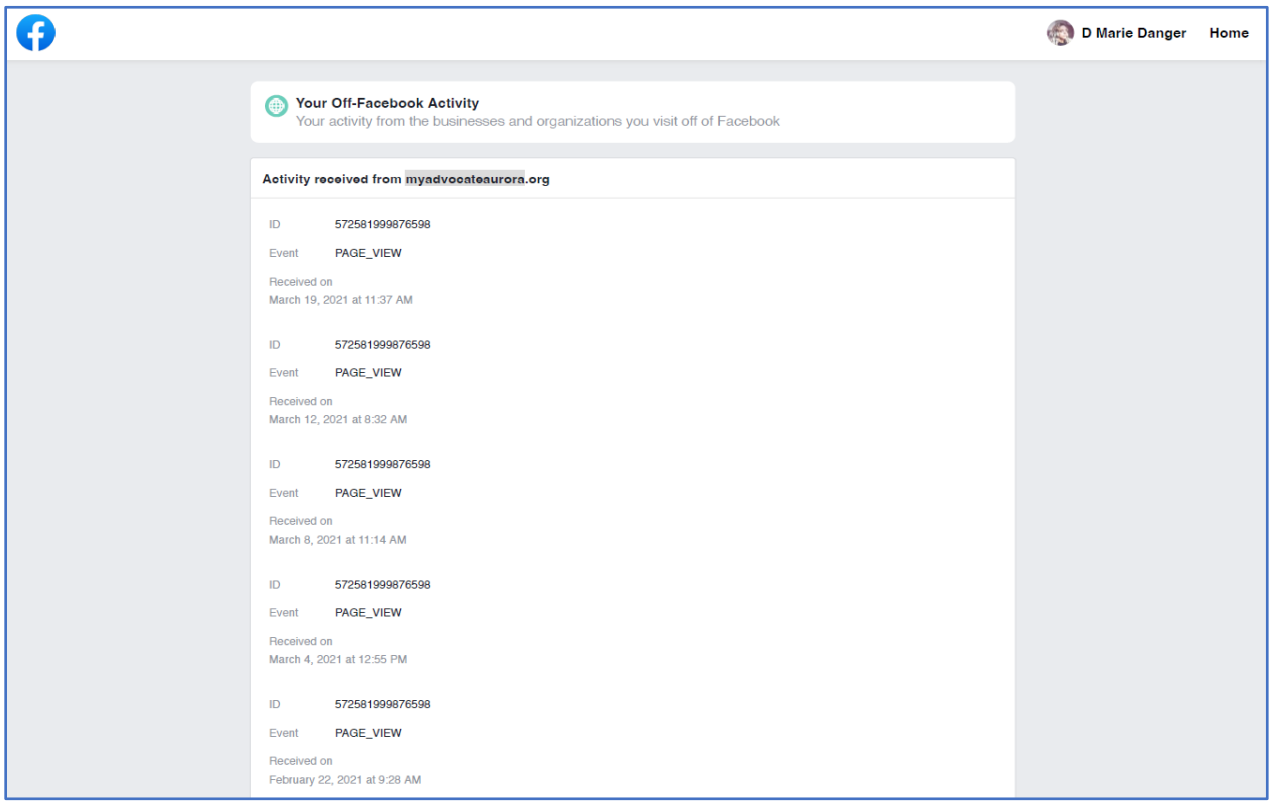
Pixel from www.aurorahealthcare.org ("Pixel 2")

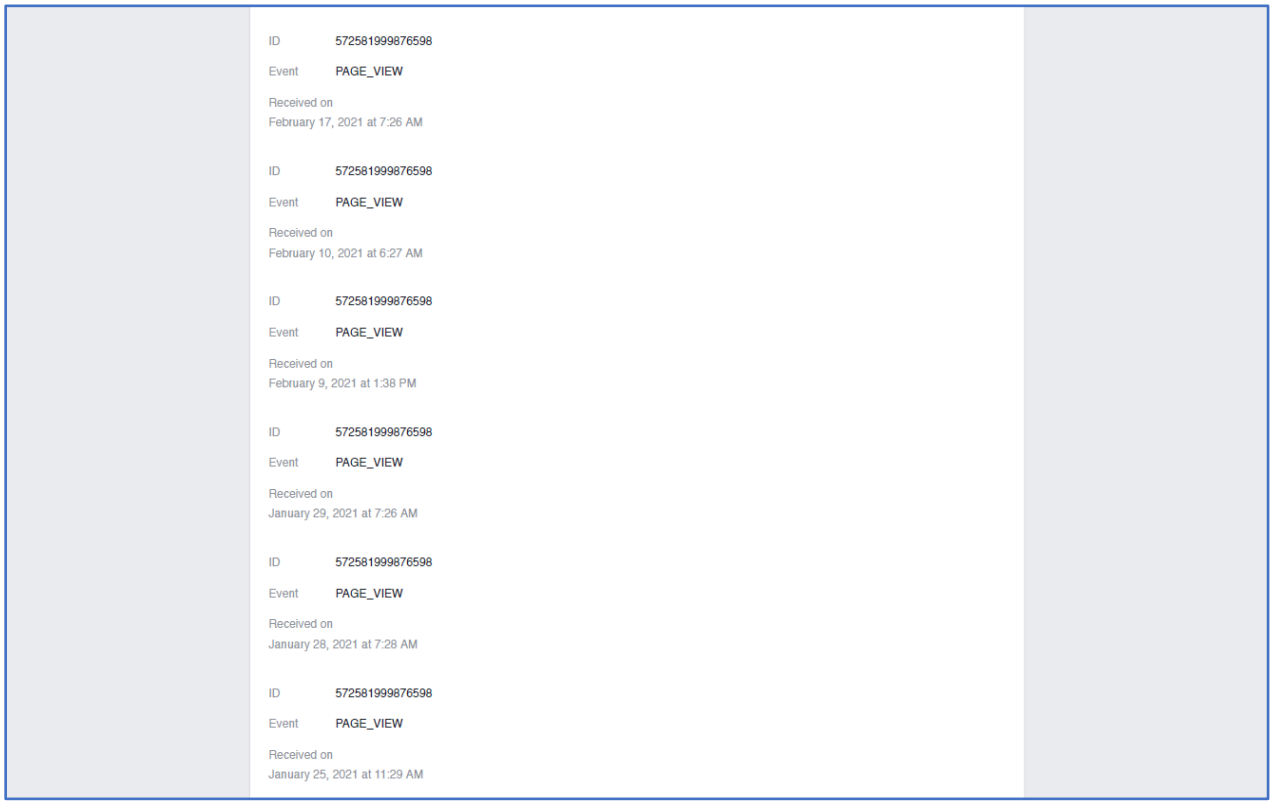


152. As shown above, Plaintiff Danger's Off-Facebook Download activity shows Defendant's Pixel ID Number 5725819999876598 was contained in Defendant's webpage www.aurorahealthcare.org (a different webpage from www.advocateaurorahealth.org) and communicated with Plaintiff Danger's Facebook on the following dates and times:

- April 7, 2022 at 7:38 am

Pixel from www.advocateaurora.com





153. As shown above, Plaintiff Danger's Off-Facebook Download activity shows Defendant's Pixel ID Number 5725819999876598 was contained in Defendant's webpage www.myadvocateaurora.org and communicated with Plaintiff Danger's Facebook on the following dates and times:

- January 25, 2021 at 11:29 am;
- January 28, 2021 at 7:28 am;
- January 29, 2021 at 7:26 am;
- February 9, 2021 at 1:38 pm;
- February 10, 2021 at 6:27 am;
- February 17, 2021 at 7:26 am;
- February 22, 2021 at 9:28 am;
- March 4, 2021 at 12:56 pm;
- March 8, 2021 at 11:14 am;
- March 12, 2021 at 8:30 am; and
- March 19, 2021 at 11:37 am

154. Notably, www.myadvocateaurora.org contains the LiveWell App and access to the MyChart Portal. On the homepage, it provides links to "billing," "message your doctor," "safecheck screening," "get your test results," "manage appointments," "start a video visit," and "classes and events."

155. From January to March 2021, Plaintiff Danger sought and received medical treatment regarding wellness checkups for prescription medication and female wellness checks. During that timeframe, Plaintiff communicated with her treatment providers regarding medical

conditions, medical records, lab results, and used the LiveWell App and MyChart Portal to schedule appointments and procedures.

156. The Off-Facebook Activity Downloads show Defendant's Tracking Pixel communicating with Plaintiff's Facebook account on the days that Plaintiff used Defendant's Website to communicate Private Information.

157. The Off-Facebook Activity Downloads indicate Defendant's Website transmitted and disclosed Plaintiff's Private Information to Facebook because it shows the real-time transmission of Private Information from Defendant's Website to Facebook on dates and times that Plaintiff Danger communicated Private Information to Defendant.

Defendant's Privacy Policies and Promises

158. Defendant's Privacy Policies allow for the disclosure of patient information in the following settings: (1) patient treatment; (2) running their organization; (3) billing; and (4) as enabled by law.[29]

159. Defendant's Privacy Policies unequivocally state Defendant will not share Plaintiffs' and Class Members' Private Information for marketing purposes unless patients provide written permission.[30]

160. Plaintiffs and Class Members have not provided Defendant with written permission to share their Private Information for marketing purposes.

161. Despite Defendant's acknowledgement that it will not share Plaintiffs' and Class Members' Private Information, Defendant, in fact, shared Plaintiffs' and Class Members' Private Information via the Tracking Pixel.

[29] https://www.advocateaurorahealth.org/notice-of-privacy-practices/ (Last visited: January 19, 2023).
[30] *Id.*

162. Specifically, Defendant transmitted and/or disclosed Plaintiffs' and Class Members' Private Information to third parties, like Facebook and Google, without Plaintiffs' and Class Members' consent or written permission.

163. In doing so, Defendant intended to improve and save costs on its marketing campaign, improve its data analytics, attract new patients, and market new services and/or treatments to its existing patients.

164. In simple terms, Defendant violated its own Privacy Policy—i.e., the Privacy Policy that Plaintiffs and Class Members relied upon—in order to bolster its profits.

Defendant Violated HIPAA Standards

165. Under Federal Law, a healthcare provider may not disclose personally identifiable, non-public medical information about a patient, a potential patient, or household member of a patient for marketing purposes without the patients' express written authorization.[31]

166. Guidance from the United States Department of Health and Human Services instructs healthcare providers that patient status alone is protected by HIPAA.

167. In Guidance regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act Privacy Rule, the Department instructs:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data… If such information was listed with health condition, health care provision, or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.[32]

[31] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).
[32] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (last visited Nov. 3, 2022)

168. In its guidance for Marketing, the Department further instructs:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, *covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list*. (Emphasis added).[33]

169. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA covered entities and business associates ("regulated entities") under the HIPAA Privacy, Security, and Breach Notification Rules ("HIPAA Rules") when using online tracking technologies ("tracking technologies").[34]

170. The Bulletin expressly provides that "[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."

171. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Tracking Pixel.

Defendant Violated Industry Standards

172. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

173. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications.

174. AMA Code of Ethics Opinion 3.1.1 provides:

[33] https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf (last visited Nov. 3, 2022)
[34] *See* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

> Protecting information gathered in association with the care of the patient is a core value in health care… Patient privacy encompasses a number of aspects, including, … personal data (informational privacy)

175. AMA Code of Medical Ethics Opinion 3.2.4 provides:

> Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

176. AMA Code of Medical Ethics Opinion 3.3.2 provides:

> Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically…must…:(c) release patient information only in keeping ethics guidelines for confidentiality.

Plaintiffs' and Class Members' Expectation of Privacy

177. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

178. Indeed, at all times when Plaintiffs and Class Members provided their PII and PHI to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

IP Addresses are Personally Identifiable Information

179. On information and belief, through the use of the Tracking Pixels on Defendant's Website, Defendant also disclosed and otherwise assisted Facebook, Google, and/or other third parties with intercepting Plaintiffs' and Class Members' Computer IP addresses.

180. An IP address is a number that identifies the address of a device connected to the Internet.

181. IP addresses are used to identify and route communications on the Internet.

182. IP addresses of individual Internet users are used by Internet service providers, Websites, and third-party tracking companies to facilitate and track Internet communications.

183. Facebook tracks every IP address ever associated with a Facebook user.

184. Google also tracks IP addresses associated with Internet users.

185. Facebook, Google, and other third-party marketing companies track IP addresses for use in tracking and targeting individual homes and their occupants with advertising by using IP addresses.

186. Under HIPAA, an IP address is considered personally identifiable information:

a. HIPAA defines personally identifiable information to include "any unique identifying number, characteristic or code" and specifically lists the example of IP addresses. *See* 45 C.F.R. § 164.514 (2).

b. HIPAA further declares information as personally identifiable where the covered entity has "actual knowledge that the information to identify an individual who is a subject of the information." 45 C.F.R. § 164.514(2)(ii); *See* also, 45 C.F.R. § 164.514(b)(2)(i)(O).

187. Consequently, by disclosing IP addresses, Defendant's business practices violated HIPAA and industry privacy standards.

Defendant was Enriched and Benefitted from the Use of the Pixel and Unauthorized Disclosures

188. The sole purpose of the use of the Tracking Pixel on Defendant's Website was marketing and profits.

189. In exchange for disclosing the Private Information of its patients, Defendant is compensated by third parties, like Facebook and Google, in the form of enhanced advertising services and more cost-efficient marketing on Facebook.

190. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions.

191. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients, including Plaintiffs and Class Members.

192. By utilizing the Pixel, the cost of advertising and retargeting was reduced, thereby benefitting Defendant.

Defendant Unlawfully Disclosed Plaintiffs' Private Information to Facebook and other Third Parties

Plaintiff Shyanne John

193. Plaintiff Shyanne John entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff John disclosed her Private Information to Defendant.

194. Plaintiff John accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

195. Plaintiff John scheduled doctor's appointments for herself via Defendant's Website.

196. Plaintiff John reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

197. Plaintiff John provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

198. As described herein, Defendant worked along with Facebook to intercept Plaintiff John's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

199. Defendant transmitted to third parties Plaintiff John's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff John and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

200. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

201. By doing so without Plaintiff John's consent, Defendant breached Plaintiff John's right to privacy and unlawfully disclosed Plaintiff John's Private Information to third parties.

202. Defendant did not inform Plaintiff John that it had shared her Private Information with Facebook until on or around October 22, 2022.

203. Plaintiff John suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

204. Plaintiff John has a continuing interest in ensuring that Plaintiff John's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff Richard Webster

205. Plaintiff Richard Webster entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Webster disclosed his Private Information to Defendant.

206. Plaintiff Webster accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

207. Plaintiff Webster scheduled doctor's appointments for himself via Defendant's Website.

208. Plaintiff Webster reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

209. Plaintiff Webster provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

210. As described herein, Defendant worked along with Facebook to intercept Plaintiff Webster's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

211. Defendant transmitted to third parties, like Facebook, Plaintiff Webster's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location;

information about providers; types of appointments or procedures; communications between Plaintiff Webster and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

212. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

213. By doing so without Plaintiff Webster's consent, Defendant breached Plaintiff Webster's right to privacy and unlawfully disclosed Plaintiff Webster's Private Information.

214. Defendant did not inform Plaintiff Webster that it had shared his Private Information with Facebook until on or around October 22, 2022.

215. Plaintiff Webster suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

216. Plaintiff Webster has a continuing interesting in ensuring that Plaintiff Webster's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff Deanna Danger

217. Plaintiff Deanna Danger entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Danger disclosed her Private Information to Defendant.

218. Plaintiff Danger accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

219. Plaintiff Danger scheduled doctor's appointments for herself via Defendant's Website.

220. Plaintiff Danger reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

221. Plaintiff Danger provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

222. As described herein, Defendant worked along with Facebook to intercept Plaintiff Danger's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

223. Defendant transmitted to third parties, like Facebook, Plaintiff Danger's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Danger and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

224. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

225. By doing so without Plaintiff Danger's consent, Defendant breached Plaintiff Danger's right to privacy and unlawfully disclosed Plaintiff Danger's Private Information.

226. Defendant did not inform Plaintiff Danger that it had shared her Private Information with Facebook until on or around October 22, 2022.

227. Plaintiff Danger suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

228. Plaintiff Danger has a continuing interesting in ensuring that Plaintiff Danger's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff James Gabriel

229. Plaintiff James Gabriel entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Gabriel disclosed his Private Information to Defendant.

230. Plaintiff Gabriel accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

231. Plaintiff Gabriel scheduled doctor's appointments for himself via Defendant's Website.

232. Plaintiff Gabriel reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

233. Plaintiff Gabriel provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

234. As described herein, Defendant worked along with Facebook to intercept Plaintiff Gabriel's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

235. Defendant transmitted to third parties, like Facebook, Plaintiff Gabriel's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Gabriel and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

236. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

237. By doing so without Plaintiff Gabriel's consent, Defendant breached Plaintiff Gabriel's right to privacy and unlawfully disclosed Plaintiff Gabriel's Private Information.

238. Defendant did not inform Plaintiff Gabriel that it had shared his Private Information with Facebook until on or around October 22, 2022.

239. Plaintiff Gabriel suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of

the Private Information; (v) statutory damages; and (v) the continued and ongoing risk to their Private Information.

240. Plaintiff Gabriel has a continuing interesting in ensuring that Plaintiff Gabriel's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff Katrina Jones

241. Plaintiff Katrina Jones entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Jones disclosed her Private Information to Defendant.

242. Plaintiff Jones accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

243. Plaintiff Jones scheduled doctor's appointments for herself via Defendant's Website.

244. Plaintiff Jones reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

245. Plaintiff Jones provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

246. As described herein, Defendant worked along with Facebook to intercept Plaintiff Jones' communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

247. Defendant transmitted to third parties, like Facebook, Plaintiff Jones' Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Jones and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

248. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

249. By doing so without Plaintiff Jones' consent, Defendant breached Plaintiff Jones' right to privacy and unlawfully disclosed Plaintiff Jones' Private Information.

250. Defendant did not inform Plaintiff Jones that it had shared her Private Information with Facebook until on or around October 22, 2022.

251. Plaintiff Jones suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

252. Plaintiff Jones has a continuing interesting in ensuring that Plaintiff Jones' Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff Derek Harris

253. Plaintiff Derrick Harris entrusted his Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Harris disclosed his Private Information to Defendant.

254. Plaintiff Harris accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

255. Plaintiff Harris scheduled doctor's appointments for himself via Defendant's Website.

256. Plaintiff Harris reasonably expected that his communications with Defendant via the Website were confidential, solely between himself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

257. Plaintiff Harris provided his Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

258. As described herein, Defendant worked along with Facebook to intercept Plaintiff Harris' communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

259. Defendant transmitted to third parties, like Facebook, Plaintiff Harris' Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff John and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

260. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

261. By doing so without Plaintiff Harris' consent, Defendant breached Plaintiff Harris' right to privacy and unlawfully disclosed Plaintiff Harris' Private Information.

262. Defendant did not inform Plaintiff Harris that it had shared his Private Information with Facebook until on or around October 22, 2022.

263. Plaintiff Harris suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

264. Plaintiff Harris has a continuing interesting in ensuring that Plaintiff Harris' Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff Amber Smith

265. Plaintiff Amber Smith entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Smith disclosed her Private Information to Defendant.

266. Plaintiff Smith accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

267. Plaintiff Smith scheduled doctor's appointments for herself via Defendant's Website.

268. Plaintiff Smith reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

269. Plaintiff Smith provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

270. As described herein, Defendant worked along with Facebook to intercept Plaintiff Smith's communications, including those that contained Private Information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

271. Defendant transmitted to third parties, like Facebook, Plaintiff Smith's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff Smith and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

272. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

273. By doing so without Plaintiff Smith's consent, Defendant breached Plaintiff Smith's right to privacy and unlawfully disclosed Plaintiff Smith's Private Information.

274. Defendant did not inform Plaintiff Smith that it had shared her Private Information with Facebook until on or around October 22, 2022.

275. Plaintiff Smith suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

276. Plaintiff Smith has a continuing interesting in ensuring that Plaintiff Smith's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

Plaintiff Bonnie Laporte

277. Plaintiff Bonnie Laporte entrusted her Private Information to Defendant. As a condition of receiving Defendant's services, Plaintiff Laporte disclosed her Private Information to Defendant.

278. Plaintiff Laporte accessed Defendant's Website to receive healthcare services from Defendant and at Defendant's direction.

279. Plaintiff Laporte scheduled doctor's appointments for herself via Defendant's Website.

280. Plaintiff Laporte reasonably expected that her communications with Defendant via the Website were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

281. Plaintiff Laporte provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

282. As described herein, Defendant worked along with Facebook to intercept Plaintiff Laporte's communications, including those that contained Private and confidential information. Defendant willfully facilitated these interceptions without Plaintiff's knowledge, consent, or express written authorization.

283. Defendant transmitted to third parties, like Facebook, Plaintiff Laporte's Private Information, including, but not limited to, the following: IP addresses; dates, times, and/or locations of scheduled appointments; proximity to an Advocate Aurora Health location; information about providers; types of appointments or procedures; communications between Plaintiff John and others through MyChart, which may have included first and last names and medical record numbers; and insurance information.

284. As a "redundant" measure to ensure Plaintiff's Private Information was successfully transmitted to third parties like Facebook, Defendant implemented server-based workarounds like Conversions API to send Plaintiff's Private Information from electronic storage on Defendant's server directly to Facebook.

285. By doing so without Plaintiff Laporte's consent, Defendant breached Plaintiff Laporte's right to privacy and unlawfully disclosed Plaintiff Laporte's Private Information.

286. Defendant did not inform Plaintiff Laporte that it had shared her Private Information with Facebook until on or around October 22, 2022.

287. Plaintiff Laporte is diagnosed with medical conditions that she disclosed on Defendant's Website. After submitting this information, Plaintiff Laporte noticed Facebook advertisements targeted towards the medical information that she disclosed via Defendant's Website.

288. Plaintiff Laporte suffered damages in form of (i) invasion of privacy; (ii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the disclosure of Private Information; (iii) loss of benefit of the bargain; (iv) diminution of value of the Private Information; (v) statutory damages; and (vi) the continued and ongoing risk to their Private Information.

289. Plaintiff Laporte has a continuing interesting in ensuring that Plaintiff Laporte's Private Information – which, upon information and belief, remains backed up in Defendant's possession – is protected and safeguarded from future unauthorized disclosure.

TOLLING

290. Any applicable statute of limitations has been tolled by the "delayed discovery" rule. Plaintiffs did not know (and had no way of knowing) that Plaintiffs' Private Information was intercepted and unlawfully disclosed because Defendant kept this information secret until Defendant's disclosure in October 2022.

CLASS ACTION ALLEGATIONS

291. Plaintiffs brings this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

292. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website, LiveWell App, and MyChart patient portal.**

293. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs John, Webster, Danger, and Gabriel (the "Wisconsin Plaintiffs") assert claims on behalf of a separate subclass, defined as follows:

All individuals residing in Wisconsin whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website, LiveWell App, and MyChart patient portal (the "Wisconsin Class").

294. In addition to the claims asserted on behalf of the Nationwide Class, Plaintiffs Jones, Harris, Smith, and Laporte (the "Illinois Plaintiffs") assert claims on behalf of a separate subclass, defined as follows:

All individuals residing in Illinois whose Private Information was disclosed to a third party without authorization or consent through the Tracking Pixel on Defendant's Website, LiveWell App, and MyChart patient portal (the "Illinois Class").

295. Excluded from the Class and Subclasses are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

296. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

297. Numerosity, Fed R. Civ. P. 23(a)(1). The Class Members for each proposed Class are so numerous that joinder of all members is impracticable. Upon information and belief, there are over 3,000,000 million individuals whose Private Information may have been improperly accessed by Facebook and/or Google, and the Class is identifiable within Defendant's records.

298. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3). Questions of law and fact common to each Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant violated its Privacy Policies by disclosing the PII and PHI of Plaintiffs and Class Members to Facebook, Google, and/or additional third parties.

d. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII and PHI would be disclosed to third parties;

e. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

f. Whether Defendant adequately addressed and fixed the practices which permitted the disclosure of patient PHI and PII;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members;

h. Whether Defendant violated the consumer protection statutes invoked herein;

i. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Defendant knowingly made false representations as to its data security and/or Privacy Policies practices;

k. Whether Defendant knowingly omitted material representations with respect to its data security and/or Privacy Policies practices; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of Defendant's disclosure of their PII and PHI.

299. Typicality, Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other

Class Members because all had their PII and PHI compromised as a result of Defendant's incorporation of the Facebook Pixel, due to Defendant's misfeasance.

300. Adequacy, Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiffs has suffered are typical of other Class Members. Plaintiffs has also retained counsel experienced in complex class action litigation, and Plaintiffs intends to prosecute this action vigorously.

301. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

302. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect

to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

303. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

304. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

305. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

306. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the practices complained of herein, and Defendant may continue to act unlawfully as set forth in this Complaint.

307. Further, Defendant has acted or refused to act on grounds generally applicable to each Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

308. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information;

b. Whether Defendant owed a legal duty to not disclose Plaintiffs' and Class Members' Private Information with respect to Defendant's Privacy Policies;

c. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

d. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

e. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information would be disclosed to third parties;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed to third parties; and

g. Whether Class Members are entitled to actual, consequential, and/or nominal

damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

309. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

COUNT I
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

310. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

311. The Private Information of Plaintiffs and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

312. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

313. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

314. The unauthorized disclosure and/or acquisition by a third party of Plaintiffs' and Class Members' Private Information via the use of the Tracking Pixel by Defendant is highly offensive to a reasonable person.

315. Defendant's willful and intentional disclosure of Plaintiffs' and Class Members' Private Information constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

316. Defendant's conduct constitutes an intentional physical or sensory intrusion on

Plaintiffs' and Class Members' privacy because Defendant facilitated Facebook's simultaneous eavesdropping and wiretapping of confidential communications.

317. Defendant failed to protect Plaintiffs' and Class Members' Private Information and acted knowingly when it incorporated the Tracking Pixel into its Website because it knew the functionality and purpose of the Tracking Pixel.

318. Because Defendant intentionally and willfully incorporated the Tracking Pixel into its Website and encouraged patients to use that Website for healthcare purposes, Defendant had notice and knew that its practices would cause injury to Plaintiffs and Class Members. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiffs and the Class Members was disclosed to a third party without authorization, causing Plaintiffs and the Class to suffer damages.

319. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, loss of time and opportunity costs, punitive damages, plus prejudgment interest, and costs.

320. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant and still in the possession of Facebook, Google, and/or other third parties, and the wrongful disclosure of the information cannot be undone.

321. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not undo Defendant's disclosure of the information to Facebook, who on information and belief continues to possess and utilize that information.

322. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT II
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

323. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

324. Defendant benefits from the use of Plaintiffs' and Class Members' Private Information and unjustly retained those benefits at their expense.

325. Plaintiffs and Class Members conferred a benefit upon Defendant in the form of Private Information that Defendant collected from Plaintiffs and Class Members and then disclosed to third parties without authorization and proper compensation. Defendant consciously collected and used this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation.

326. Defendant unjustly retained those benefits at the expense of Plaintiffs and Class Members because Defendant's conduct damaged Plaintiffs and Class Members, all without providing any commensurate compensation to Plaintiffs and Class Members.

327. The benefits that Defendant derived from Plaintiffs and Class Members were not offered by Plaintiffs and Class Members gratuitously and rightly belong to Plaintiffs and Class Members. It would be inequitable under unjust enrichment principles in Illinois, Wisconsin, and every other state for Defendant to be permitted to retain any of the profit or other benefits wrongly derived from the unfair and unconscionable methods, acts, and trade practices alleged in this

Complaint.

328. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

329. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

330. When Plaintiffs and Class Members provided their user data to Defendant in exchange for services, they entered into an implied contract pursuant to which Defendant agreed to safeguard and not disclose their Private Information without consent.

331. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

332. Plaintiffs and Class Members would not have entrusted Defendant with their Private Information in the absence of an implied contract between them and Defendant obligating Defendant to not disclose Private Information without consent.

333. Defendant breached these implied contracts by disclosing Plaintiffs' and Class Members' Private Information to third parties, *i.e.*, Facebook and/or Google.

334. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class Members would not have used Defendant's services, or would have paid substantially for these services, had they known their Private Information would be disclosed.

335. Plaintiffs and Class Members are entitled to compensatory and consequential

damages as a result of Defendant's breach of implied contract.

COUNT IV
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Nationwide Class)

336. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

337. Medical providers have a duty to their patients to keep non-public medical information completely confidential.

338. Plaintiffs and Class Members had reasonable expectations of privacy in their communications exchanged with Defendant, including communications exchanged on Defendant's Website and on Defendant's MyChart portal.

339. Plaintiffs' and Class Members' reasonable expectations of privacy in the communications exchanged with Defendant were further buttressed by Defendant's express promises in its Privacy Policies.

340. Contrary to its duties as a medical provider and its express promises of confidentiality, Defendant deployed the Tracking Pixel to disclose and transmit Plaintiffs' Private Information and the contents of their communications exchanged with Defendant to third parties.

341. The third-party recipients included, but were not limited to, Facebook and Google.

342. Defendant's disclosures of Plaintiffs' and Class Members' Private Information were made without their knowledge, consent, or authorization, and were unprivileged.

343. The harm arising from a breach of provider-patient confidentiality includes erosion of the essential confidential relationship between the healthcare provider and the patient.

344. As a direct and proximate cause of Defendant's unauthorized disclosures of patient personally identifiable, non-public medical information, and communications, Plaintiffs and Class

members were damaged by Defendant's breach in that:

a. Sensitive and confidential information that Plaintiffs and Class members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the provider-patient relationship;

c. Defendant took something of value from Plaintiffs and Class members and derived benefit therefrom without Plaintiffs' and Class members' knowledge or informed consent and without compensating Plaintiffs for the data;

d. Plaintiffs and Class members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality;

e. Defendant's actions diminished the value of Plaintiffs' and Class members' Private Information; and

f. Defendant's actions violated the property rights Plaintiffs and Class members have in their Private Information.

345. Plaintiffs and Class Members are therefore entitled to general damages for invasion of their rights in an amount to be determined by a jury and nominal damages for each independent violation.

COUNT V
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA")
18 U.S.C. § 2511(1) *et seq*.
UNAUTHORIZED INTERCEPTION, USE, AND DISCLOSURE
(On Behalf of Plaintiffs and the Nationwide Class)

346. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

347. The ECPA protects both sending and receipt of communications.

348. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

349. The transmissions of Plaintiffs' PII and PHI to Defendant's Website qualifies as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

350. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

351. **Content.** The ECPA defines content, when used with respect to electronic communications, to "include[] *any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

352. **Interception.** The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

353. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiffs' and Class Members' browsers;

b. Plaintiffs' and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Pixel Code deployed by Defendant to effectuate the sending and acquisition of patient communications

354. By utilizing and embedding the Pixel on its Website, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

355. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Tracking Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such Facebook and Google.

356. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs' and Class Members' regarding PII and PHI, treatment, medication, and scheduling.

357. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

358. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

359. **Unauthorized Purpose**. Defendant intentionally intercepted the contents of

Plaintiffs' and Class Members' electronic communications for the purpose of committing a tortious act in violation of the Constitution or laws of the United States or of any State – namely, invasion of privacy, among others.

360. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' PII and PHI for financial gain.

361. Defendant was not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

362. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiffs' privacy via the Pixel tracking code.

363. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

364. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Website, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions, including as described above the following: (1) a knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person; and (2) violation of the Wisconsin Deceptive Trade Practices Act and Illinois Consumer Fraud Act.

COUNT VI
VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT UNAUTHORIZED DIVULGENCE BY ELECTRONIC COMMUNICATIONS SERVICE 18 U.S.C. § 2511(3)(a) (On Behalf of Plaintiffs and the Nationwide Class)

365. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

366. The ECPA Wiretap statute provides that "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

367. **Electronic Communication Service**. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

368. Defendant's Website and/or MyChart Portal are electronic communication services. Both services provide to users thereof the ability to send or receive electronic communications. In the absence of Defendant's Website and MyChart Portal, internet users could not send or receive communications regarding Plaintiffs' and Class Members' PII and PHI.

369. **Intentional Divulgence**. Defendant intentionally designed the Tracking Pixel and was or should have been aware that, if misconfigured, it could divulge Plaintiffs' and Class Members' PII and PHI.

370. **While in Transmission**. Upon information and belief, Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications was contemporaneous with their exchange with Defendant's Website and/or MyChart Portal, to which they directed their communications.

371. Defendant divulged the contents of Plaintiffs' and Class Members' electronic communications without authorization. Defendant divulged the contents of Plaintiffs' and Class Members' communications to Facebook without Plaintiffs' and Class Members' consent and/or authorization.

372. **Exceptions do not apply**. In addition to the exception for communications directly to an ECS or an agent of an ECS, the Wiretap Act states that "[a] person or entity providing electronic communication service to the public may divulge the contents of any such communication as follows:

a. "as otherwise authorized in section 2511(2)(a) or 2517 of this title;"

b. "with the lawful consent of the originator or any addressee or intended recipient of such communication;"

c. "to a person employed or authorized, or whose facilities are used, to forward such communication to its destination;" or

d. "which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency."

18 U.S.C. § 2511(3)(b)

373. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

374. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's Website and/or MyChart Portal to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's service; nor (2) necessary to the protection of the rights or property of Defendant.

375. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

376. Defendant's divulgence of the contents of user communications on Defendant's browser through the Pixel code was not done "with the lawful consent of the originator or any addresses or intended recipient of such communication[s]." As alleged above: (a) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiffs and Class Members were exchanging information.

377. Moreover, Defendant divulged the contents of Plaintiffs and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

378. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

379. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VII
VIOLATION OF TITLE II OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 18 U.S.C. § 2702, *et seq.* (STORED COMMUNICATIONS ACT) (On Behalf of Plaintiffs and the Nationwide Class)

380. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

381. The ECPA further provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

382. **Electronic Communication Service.** ECPA defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

383. Defendant intentionally procures and embeds various Plaintiffs' PII and PHI through the Pixel Code used on Defendant's Website and/or MyChart Portal, which qualifies as an Electronic Communication Service.

384. **Electronic Storage**. ECPA defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

385. Defendant stores the content of Plaintiffs' and Class Members' communications on Defendant's Website and/or MyChart Portal and files associated with it.

386. When Plaintiffs or Class Members make a Website communication and/or submission to the MyChart Portal, the content of that communication is immediately placed into storage.

387. Defendant knowingly divulges the contents of Plaintiffs' and Class Members' communications from electronic storage through workarounds including Facebook's Conversions API.

388. **Exceptions Do Not Apply**. Section 2702(b) of the Stored Communication Act provides that an electronic communication service provider "may divulge the contents of a

communication—"

a. "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

b. "as otherwise authorized in Section 2517, 2511(2)(a), or 2703 of this title;"

c. "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;"

d. "to a person employed or authorized or whose facilities are used to forward such communication to its destination;"

e. "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;"

f. "to the National Center for Missing and Exploited Children, in connection with a reported submission thereto under section 2258A."

g. "to law enforcement agency, if the contents (i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime;"

h. "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency"; or

i. "to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies Section 2523."

389. Defendant did not divulge the contents of Plaintiffs' and Class Members' communications to "addressees," "intended recipients," or "agents" of any such addressees or intended recipients of Plaintiffs and Class Members.

390. Section 2517 and 2703 of the ECPA relate to investigations by government officials and have no relevance here.

391. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication

> service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

392. Defendant's divulgence of the contents of Plaintiffs' and Class Members' communications on Defendant's Website to Facebook was not authorized by 18 U.S.C. § 2511(2)(a)(i) in that it was neither: (1) a necessary incident to the rendition of Defendant's services; nor (2) necessary to the protection of the rights or property of Defendant.

393. Section 2517 of the ECPA relates to investigations by government officials and has no relevance here.

394. Defendant's divulgence of the contents of user communications on Defendant's Website and/or MyChart Portal was not done "with the lawful consent of the originator or any addresses or intend recipient of such communication[s]." As alleged above: (a) Plaintiffs and Class Members did not authorize Defendant to divulge the contents of their communications; and (b) Defendant did not procure the "lawful consent" from the Websites or apps with which Plaintiffs and Class Members were exchanging information.

395. Moreover, Defendant divulged the contents of Plaintiffs' and Class Members' communications through the Facebook Pixel to individuals who are not "person[s] employed or whose facilities are used to forward such communication to its destination."

396. The contents of Plaintiffs' and Class Members' communications did not appear to pertain to the commission of a crime and Defendant did not divulge the contents of their communications to a law enforcement agency.

397. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may

assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; punitive damages in an amount to be determined by a jury; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT VIII
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT (CFAA)
18 U.S.C. § 1030, ET SEQ.
(On Behalf of Plaintiffs and the Nationwide Class)

398. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

399. Plaintiffs' and the Class's mobile devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

400. Defendant exceeded, and continues to exceed, authorized access to the Plaintiffs' and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

401. Defendant's conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of Plaintiffs' and the Class's private and personally identifiable data and content – including the Website visitor's electronic communications with the Website, including their mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time ("Website Communications") which were never intended for public consumption.

402. Defendant's conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV) due to the Private Information of Plaintiffs and the Class being made available to Defendant, Facebook, and/or other third parties without adequate legal privacy

protections.

403. Accordingly, Plaintiffs and the Class Members are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."18 U.S.C. § 1030(g).

COUNT IX
VIOLATION OF CONFIDENTIALITY OF PATIENT HEALTH CARE RECORDS
Wis. Stat. § 146.81, *et seq*.
(On Behalf of Plaintiffs and the Nationwide or, alternatively, the Wisconsin Class)

404. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

405. Under Wisconsin law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

406. Defendant disclosed the private and protected medical information of Plaintiffs and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

407. Defendant is a healthcare provider as defined by Wis. Stat. § 146.816(1).

408. Plaintiffs and Class Members are patients, and, as a health care provider, Advocate had and has an ongoing obligation not to disclose their Private Information.

409. The Private information disclosed by Defendant is protected health information as defined by Wis. Stat. § 146.816(f).

410. Defendant violated Wis. Stat. § 146.81, et seq. through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class. Defendant's conduct with respect to the disclosure of its patients confidential Private Information was willful and knowing because Defendant configured and implemented the digital platforms and tracking software that gave rise to the Data Breach.

411. Plaintiffs and Class Members were injured as a result of Advocate's violation of the confidentiality of patient health care law.

412. As a result of its intentional and willful disclosure of Private Information, Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, restitution, reasonable attorneys' fees and costs, and any other relief that is just and proper.

COUNT X
WISCONSIN DECEPTIVE TRADE PRACTICES ACT
Wis. Stat. §§100.18, *et seq*.
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Wisconsin Class)

413. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

414. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"), which provides that no,

> "firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

415. Plaintiffs and Class Members "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

416. Plaintiffs and Class Members relied on and had the reasonable expectation that Defendant (i.e., a healthcare network) would protect their Private Information and comply with all common law, state, and federal privacy laws designed to protect their Private Information.

417. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement

of their services in violation of the WDPTA, including, but not limited to, the following: (1) promising to protect Plaintiffs' and Class Members' Private Information via its Privacy Policies and then, in fact, knowingly, transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google; (2) unlawfully disclosing Plaintiffs' and Class Members' Private Information to third parties such as Facebook and Google; (3) failing to disclose or omitting material facts that that Plaintiffs' and Class Members' Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs' and Class Members' consent in transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs' and Class Members' Private Information.

418. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Tracking Pixel and also knew the Pixel would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

419. Defendant intended that Plaintiffs and the Wisconsin Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

420. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiffs and Class Members have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

421. As a result of Defendant's wrongful conduct, Plaintiffs and Class Members were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient

security to keep their PII and PHI from being hacked and taken and misused by others.

422. As a direct and proximate result of Defendant's violations of the WDTPA, Plaintiffs and the Wisconsin Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiffs and the Wisconsin Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

423. Pursuant to Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5), Plaintiffs and Class Members are entitled to reasonable attorney fees and costs, punitive damages, and other relief that the Court deems proper.

COUNT XI
VIOLATION OF STATUTORY DUTY TO MAINTAIN CONFIDENTIALITY OF PATIENT HEALTHCARE RECORDS
Illinois Stat. § 410 ILCS 50, *et seq*.
(On Behalf of Illinois Plaintiffs and the Illinois Class)

424. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

425. Under Illinois law all patient health care records must remain confidential and patient health care records may only be released to a person upon the informed consent of the patient, or as authorized by the patient.

426. Defendant disclosed the private and protected medical information of Plaintiffs and Class Members to unauthorized third parties without their knowledge, consent, or authorization.

427. Defendant is a healthcare services corporation and provider as defined by 410 ILCS 501 2.02 and 2.03.

428. Plaintiffs and Class Members are patients, and, as a health care provider, Advocate had and has an ongoing obligation not to disclose their Private Information.

429. The Private information disclosed by Defendant is protected health information under the Illinois Medical Patient Rights Act.

430. Defendant violated 410 ILCS 50, *et seq.*, through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class when conducting its marketing research program with the assistance of Facebook and other third-party search engines. Defendant's conduct with respect to the disclosure of its patients confidential Private Information was willful and knowing because Defendant configured and implemented the digital platforms and tracking software that gave rise to the Breach.

431. Plaintiffs and Class Members were injured as a result of Defendant's violation of the confidentiality of the Medical Patients' Rights Act, which imposed a duty of confidentiality on Defendant.

432. As a result of its intentional and willful disclosure of Plaintiffs and Class Members' Private Information, Defendant is liable to Plaintiffs and Class Members for damages, whether nominal or actual and punitive damages.

COUNT XII
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA")
815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On behalf of Illinois Plaintiffs and the Illinois Class)

433. Plaintiffs repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

434. Plaintiffs and the Illinois Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs, the Illinois Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

435. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

436. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including, but not limited to, the following: (1) promising to protect Plaintiffs' and Class Members' Private Information via its Privacy Policies and then, in fact, knowingly, transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google; (2) unlawfully disclosing Plaintiffs' and Class Members' Private Information to third parties such as Facebook and Google; (3) failing to disclose or omitting material facts that that Plaintiffs' and Class Members' Private Information would be disclosed to third parties; (4) failing to obtain Plaintiffs' and Class Members' consent in transmitting Plaintiffs' and Class Members' Private Information to third parties, such as Facebook and Google; and (5) knowingly violating industry and legal standards regarding the protection of Plaintiffs' and Class Members' Private Information.

437. These actions also constitute deceptive and unfair acts or practices because Defendant knew its Website contained the Pixel and also knew the Pixel would be unknown and/or not easily discoverable by Plaintiffs and Class Members.

438. Defendant intended that Plaintiffs and the Illinois Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with

Defendant's offering of goods and services.

439. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Illinois Class. Plaintiffs and the Illinois Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

440. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Illinois Class of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/1, *et seq*.

441. As a result of Defendant's wrongful conduct, Plaintiffs and the Illinois Class were injured in that they never would have provided their PII and PHI to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII and PHI from being hacked and taken and misused by others.

442. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and the Illinois Class have suffered harm, including actual instances of identity theft; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiffs and the Illinois Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII and PHI; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

443. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Illinois Plaintiffs and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees

as a result of Defendant's violations of the CFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiffs and their Counsel to represent such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members:

D. For an award of damages, including, but not limited to, actual, consequential, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

444. Plaintiffs hereby demand that this matter be tried before a jury

Date: January 23, 2022

Respectfully submitted,

/s/ Terence R. Coates
Terence R. Coates
Dylan J. Gould
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
dgould@msdlegal.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Interim Co-Lead Class Counsel

David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Joseph M. Lyon
THE LYON LAW FIRM, LLC
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

Bryan L. Bleichner
Philip J. Krzeski
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone:(612)339-7300
Fax:(612)336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Nola J. Hitchcock
CROSS LAW FIRM, S.C.
WI State Bar No. 1015817
Marcy C. Flanner
WI State Bar No. 1013095
845 North 11th St.
Lawyers' Building
Milwaukee, Wisconsin 53233
Tel: (414) 224-0000
Fax: (414) 273-7055
njhcross@crosslawfirm.com
mflanner@crosslawfirm.com

Stephen R. Basser*
BARRACK RODOS & BACINE
Calif. State Bar No. 121950
E-mail: sbasser@barrack.com
Samuel M. Ward*
Calif. State Bar No. 216562
E-mail: sward@barrack.com
One America Plaza
600 West Broadway, Ste. 900
San Diego, California 92101

John Emerson*
EMERSON FIRM LLP
2500 Wilcrest, Ste. 300
Dallas, Texas 77042
jemerson@emersonfirm.com
Phone: (800) 551-8649
Fax: (501) 286-4659

Counsel for Plaintiffs and Putative Classes

**Bar application forthcoming*